Aboriginal and Torres Strait Islander eHealth

NACCHO eHealth

Health Professional's Guide

FAQ's, Resources and Support

ACCHS sites to PCEHR

Version 0.4 - DRAFT
8 April 2013

Document Information

Approver	Project Board
Owner	*Project Manager*
Contact	*Same as Owner*

Version History

[Lists the reviews undertaken to the document]

Date	Version	Name	Comments / Type of review
8 April 2013	0.1	Jonathon Siemers Nicolle Marchant	Draft Guide
8 May 2013	0.2	Jonathon Siemers Nicolle Marchant	Changes to entire document
24 June 2013	0.3	Jonathon Siemers Nicolle Marchant	New template applied
25 June 2013	0.4	Jonathon Siemers Nicolle Marchant	Changes to pages 15 - 21

Version 0.4 to be endorsed by the project board.

Table of Contents

Document Information 2

Version History 2

Important Note 4

7. FAQ's 5

7.1. General 5

7.1.1. How will the eHealth record system work? 5

7.1.2. Does an eHealth record replace existing records? 5

7.1.3. Who is eligible for an eHealth record? 5

7.1.4. What information can an eHealth record contain? 5

7.1.5. What is the physical form of the eHealth record? 6

7.2. Registering for an eHealth Record 6

7.2.1. How can patients register? 6

7.2.2 How can I participate in the eHealth record system? 7

7.2.3. How does a healthcare organisation register for the eHealth record system? 7

7.2.4. How do I access the eHealth record system? 8

7.2.5. What is the benefit of upgrading to Clinical Information System [CIS] desktop software? 8

7.2.6. What are Healthcare Identifiers? 8

7.2.7. How do I get an HPI-I or HPI-O? 9

7.2.8. Is my HPI-I unique? What if I work for more than one healthcare organisation? 9

7.2.9. I have obtained my HPI-I from AHPRA, but where do I obtain an HPI-O? 9

7.2.10. What is a National Authentication Service for Health [NASH] individual Public Key Infrastructure [PKI] certificate? 9

7.3. Managing a patient's eHealth record 10

7.3.1. Will I have access to everything in a patient's record? 10

7.3.2. What does this mean for my existing records? 10

7.3.3. Can I import data from the eHealth record system back into my own local clinical information system? 10

7.3.4. Are patients able to read what doctors and other healthcare professionals write about them in full? 11

7.3.5. Once the information is in the eHealth record system, how can I be sure that it is up to date? 11

7.3.6. Is there a log showing who has looked at eHealth records? 11

7.3.7. What about in an emergency? 11

7.3.8. Can a patient enter their own health information into their eHealth record? 12

7.3.9. When I view a patient's eHealth record, will there be any indication that certain documents have been classified as confidential or not readable? 12

7.3.10. If a patient chooses to withhold information about psychiatric history, will the medications the patient may be taking be visible? 12
7.3.11. What are my obligations if I identify an error in a patient's eHealth record? 12
7.3.12. Can lists of medications in the eHealth record be altered? 13
7.3.13. Can a patient have more than one nominated provider, e.g. a GP and a renal physician? 13
7.3.14. Will the eHealth record system be available on smart devices [e.g. iPad, tablet, smart phone]? 13
7.3.15. How will consent be managed with children? 13
7.3.16 What clinical safeguards are being developed as part of the eHealth record system? 14
7.3.17. How can I be sure that health information will be secure? 14
8. Helpdesk Contact Details 15
8.1. Related Resources 17
9. Key Definitions 19
10. Acronyms and Abbreviations 22

Important Note

This guide does not replace the advice, guidance and support provided by your software vendor.

The new eHealth features will include the ability for your health service to share clinical patient data electronically [inbound and outbound], possibly for the first time. As with all eHealth systems there is a small risk of unintended consequences if not implemented and operated correctly. This risk should be lower than at present as the new healthcare identifiers will act as a key to correctly match patient, practitioner and health service data.

In addition, as the new eHealth features require your health services computer systems to access external online services via the Internet, if not done already, you should also:

- Review the IT security arrangements in your health service and take action to address any shortcomings or areas of risk; and
- Review the reliability and performance of your health services internet connection and consider upgrading if warranted.

It is recommended that you seek advice and support from your software vendor or other organisation that provides you with IT and/or eHealth support. NACCHO or your Medicare Local may also be able to provide assistance or services to support implementing the new eHealth features in your health service.

7. FAQ's

7.1. General

7.1.1. How will the eHealth record system work?

The eHealth record system provides access to key health information drawn from a patient's health records. With the patient's consent, this information can be quickly shared between healthcare organisations and other healthcare professionals involved in the patient's care.

Over time, an eHealth record will grow to contain a summary of a patient's key healthcare events and activities, including medical history, allergies and current medications. The system is designed to be integrated into existing local clinical information systems.

7.1.2. Does an eHealth record replace existing records?

eHealth records will not replace existing medical records. Healthcare professionals will continue to take and review clinical notes. More detailed patient information will be available on local clinical information systems, as per current practice.

The eHealth record system provides an active online record that follows patients as they move through Australia's health system, and includes important clinical and treatment information.

It is expected that, in the future, the availability of eHealth records will save healthcare professionals valuable time.

7.1.3. Who is eligible for an eHealth record?

People seeking health care in Australia are eligible for an eHealth record. Registration for an eHealth record is voluntary and is not required to receive health care.

7.1.4. What information can an eHealth record contain?

An eHealth record can contain two sets of information – clinical and personal. Only authorised healthcare professionals can enter information into the clinical section of a patient's eHealth record, ensuring it is clinically relevant and as accurate as possible.

Patients will have their own section in the eHealth record, separate from the clinical section, where they will be able to enter basic health information, including Indigenous status and keep notes for their own use.

As clinical software is updated to communicate with the eHealth record system, more clinical information can be added by healthcare professionals. As the system grows, an eHealth record may contain standardised versions of the following:

- Shared health summary: This will include information about a patient's medical conditions, medications they are currently taking, allergies they may have or relevant family medical history. The shared health summary is prepared by a patient's nominated provider, who can be a medical practitioner, registered nurse or Aboriginal and Torres Strait Islander health practitioner. The structure of a patient's shared health summary is underpinned by the RACGP [Royal Australian College of General Practitioners] template for a GP health summary.
- Event summary: This is a summary of a significant consultation. It can be uploaded by a healthcare professional at any participating healthcare organisation that is authorised to use the eHealth record system – such as an ACCHS, hospital or allied health clinic.
- Hospital discharge summary: This can be uploaded by healthcare professionals who have access to the eHealth record and were involved in the patient's hospital care.
- Specialist letter: When a specialist creates a specialist letter, it will be sent directly to the intended recipient, as per current practices, and a copy of the specialist letter may also be uploaded to the eHealth record system.
- eReferral letter: When a healthcare professional creates a referral, it will be sent directly to the intended recipient, as per current practices, and a copy of the referral may also be uploaded to the eHealth record system.

7.1.5. What is the physical form of the eHealth record?

An eHealth record will be held online on secure servers. Patients can choose whether or not they want to view their record online. Some patients may only make enquiries by telephone or at Department of Human Services service centres offering Medicare services. If they do want to view their eHealth record online, they can login and access it.

7.2. Registering for an eHealth Record

7.2.1. How can patients register?

People can register for an eHealth record in the following ways:

- Online
- Over the phone – by calling 1800 723 471 and selecting option one
- In person – by visiting a Department of Human Services service centre offering Medicare services
- In writing – by completing a registration application form, available from a service centre offering Medicare services or from www.ehealth.gov.au, and posting it to: Personally Controlled eHealth Record Program, GPO Box 9942, In your Capital City
- Assisted registration

7.2.2 How can I participate in the eHealth record system?

Healthcare professionals do not need to register individually for the eHealth record system. Only healthcare organisations need to register.

Healthcare organisations in Australia can register now to participate in the eHealth record system. Once an organisation is registered, authorised users in that organisation will be able to access the system via either a conformant clinical information system with an individual logon, or via the eHealth record provider portal [read only] using their PCEHR compliant digital credential.

To participate in the eHealth record system, your healthcare organisation will need to authorise you to access the system on their behalf, once it has registered with the eHealth record system.

Healthcare professionals with a Healthcare Provider Identifier – Individual [HPI-I] will be able to upload information to the clinical section of a patient's eHealth record, once their organisation has a conformant clinical information system. Authorised users who don't have an HPI-I, but are important to an individual patient's care, will be able to access that patient's eHealth record but will not be able to upload information.

To register for an HPI-I, or to find out what your HPI-I is, and to obtain a PCEHR compliant digital credential, please go to the HI Service page on the Medicare Australia website and download the appropriate application form.

If you have your own practice, you will need to register your organisation, and designate yourself as an authorised user.

7.2.3. How does a healthcare organisation register for the eHealth record system?

To register for the eHealth record system, a healthcare organisation will first need to register with the Healthcare Identifiers [HI] Service for a Healthcare Provider Identifier – Organisation [HPI-O]. They will also need to apply to the HI Service to obtain PCEHR compliant digital credentials. To register an organisation for an HPI-O and to obtain PCEHR compliant digital credentials, go to the HI Service page on the Medicare Australia website and download the appropriate application form, or go to www.ehealth.gov.au

Once an organisation has registered with the HI Service, they will need to register for the eHealth record system by completing and submitting the Application to register as a healthcare provider organisation form and the Participation agreement for healthcare provider organisation.

For more information, download the Registration booklet for healthcare organisations.

7.2.4. How do I access the eHealth record system?

If you have been authorised to access the eHealth record system on behalf of a healthcare organisation, you will be able to access the eHealth record system via either a conformant clinical information system, or via the provider portal using their PCEHR compliant digital credential.

To gain access via clinical software you will need to use registered and approved clinical information system [CIS] desktop software and have a PCEHR compliant digital credential installed. Vendors are expected to have upgraded software available shortly. Please contact your software vendor for more information.

To gain access via the provider portal, go to www.ehealth.gov.au to log in. The provider portal is a read - and download - only facility and will not enable healthcare professionals to contribute to a patient's eHealth record. Over time, if healthcare professionals and their organisations are registered, the provider portal will give them access to the information that has been entered by patients. As software vendor products progressively become available, the information contributed to the eHealth record system by registered healthcare professionals will increasingly become available to those other healthcare professionals accessing the provider portal only.

7.2.5. What is the benefit of upgrading to Clinical Information System [CIS] desktop software?

If your organisation upgrades to clinical software that is conformant with the eHealth record system, you will be able to perform additional functions such as:

- Create an event summary – This is a summary of a significant consultation. It can be uploaded by a healthcare professional at any participating healthcare organisation authorised to use the eHealth record system.
- Create a shared health summary – This is a clinical document summarising a patients' health status. The shared health summary includes information about a patient's medical conditions and medications they are currently taking, and allergies they may have. This is likely to be the first document accessed by any new healthcare professional viewing a patient's record. This document is created by the healthcare professional who is responsible for the coordinated care of the patient.

7.2.6. What are Healthcare Identifiers?

The Healthcare Identifiers [HI] Service is a national system for allocating a unique identifier to healthcare professionals, organisations and consumers. Healthcare Identifiers will help ensure consumers and healthcare professionals can have confidence that the right information is associated with the right individual at the point of care. The HI Service allocates three types of healthcare identifiers:

- Individual Healthcare Identifier [IHI] – for individuals [consumers] receiving healthcare services
- Healthcare Provider Identifier – Individual [HPI-I] – for healthcare professionals involved in providing patient care
- Healthcare Provider Identifier – Organisation [HPI-O] – for organisations that deliver health care [such as hospitals or general practices].

7.2.7. How do I get an HPI-I or HPI-O?

You can obtain a HPI-I and a HPI-O now. Healthcare professionals who are registered with the Australian Health Practitioner Regulation Agency [AHPRA] will have been be assigned a HPI-I, and AHPRA will advise them of this number.

Healthcare professionals in a field of practice not covered by AHPRA must complete an application for a HPI-I via the Department of Human Services. Go to www.medicareaustralia.gov.au, follow the link to individual healthcare provider forms and click on the application to register a healthcare professional. You can also follow the links on this page to download the forms to register your organisation for an HPI-O.

If you have not received your HPI-I, or have forgotten it, call the Healthcare Identifiers Service on 1300 361 457.

7.2.8. Is my HPI-I unique? What if I work for more than one healthcare organisation?

Your HPI-I is unique to you. You will only need one HPI-I regardless of the number of qualifications obtained or healthcare organisations for which you work.

7.2.9. I have obtained my HPI-I from AHPRA, but where do I obtain an HPI-O?

A healthcare provider organisation will need to register for an HPI-O with the HI Service [Department of Human Services]. Organisations that are eligible for an HPI-O must be an entity that has conducted, conducts, or will conduct, an enterprise that provides healthcare services.

An HPI-O may be linked to all relevant HPI-Is in the organisation. Organisations can apply directly to the HI Service by completing the application form on the Medicare Australia website.

7.2.10. What is a National Authentication Service for Health [NASH] individual Public Key Infrastructure [PKI] certificate?

A National Authentication Service for Health [NASH] individual Public Key Infrastructure [PKI] certificate is a part of the security measures put in place to protect the privacy of eHealth records and is an important part of the system. A NASH location PKI certificate is needed to authenticate healthcare professionals accessing the eHealth record system. These certificates can be loaded onto smart cards.

When you login via the provider portal, you will be automatically logged out after 15 minutes of inactivity, even if you have removed your PCEHR compliant digital credential.

Until NASH is available, the Interim Authentication Solution is a modified Department of Human Services [DHS] PKI solution which is Government-accredited, and has protection capabilities to enable trusted connections to the eHealth record system and can be used for the initial registration and set-up stages.

Software vendors can use the modified DHS PKI as an interim arrangement for connection to the eHealth record system and replace it with the NASH PKI when it becomes available. This interim solution is also referred to as PCEHR compliant digital credentials.

7.3. Managing a patient's eHealth record

7.3.1. Will I have access to everything in a patient's record?

If a patient chooses to have an eHealth record, they will be able to control what information is stored in the record and which healthcare organisations can access that information. This ability to set access control measures is a key privacy feature of the eHealth record system. While privacy is important, it is best for all information to be available to enable healthcare professionals to deliver the most appropriate care.

Only healthcare professionals from authorised Australian organisations with software that can communicate with the eHealth record system will be able to upload information to a patient's eHealth record.

7.3.2. What does this mean for my existing records?

The eHealth record system does not replace existing clinical records. It is an additional tool that provides a summary of patient information entered by healthcare professionals from different healthcare organisations. It will enable a single view of a summary of a patient's information from across the health system. It will only contain information that a patient has consented to have included in their eHealth record.

If a healthcare professional sees a new patient with an eHealth record for a consultation, with the patient's consent the healthcare professional can view their key medical information, which will save time questioning the patient or chasing missing information.

7.3.3. Can I import data from the eHealth record system back into my own local clinical information system?

A healthcare organisation that is registered for the eHealth record system will be able to copy information out of the national system into their local clinical information system.

In the early stages of implementation, this will be done manually from the web-based provider portal. In time there will be integrated access to the eHealth record system via conformant clinical information system desktop software.

7.3.4. Are patients able to read what doctors and other healthcare professionals write about them in full?

Patients can read in full everything that is added to their eHealth record. You may choose to include additional information in your own local clinical information system that is not included in the eHealth record. In any event, patients have a right under the *Privacy Act 1988 [Cth]* to access the personal information that healthcare professionals hold about them. For more information, please contact the Office of the Australian Information Commissioner or 1300 363 992.

7.3.5. Once the information is in the eHealth record system, how can I be sure that it is up to date?

All clinical documents in the eHealth record system will be accompanied by document source information stating where, when and by whom the document was created. All clinical documents will also be digitally signed by the supplying healthcare organisation to ensure they have not been modified since they were submitted. Based on the above information, a healthcare professional will then be able to make a professional judgement about the reliability of the information.

It should also be noted that healthcare organisations have an obligation to take reasonable steps so that any personal and health information uploaded to a person's eHealth record is as accurate as possible and up-to-date at the time of uploading.

7.3.6. Is there a log showing who has looked at eHealth records?

Yes. A patient's eHealth record will have a view showing the activity history related to their record. This will show when information has been added or removed as well as the organisation that viewed the record and when. Healthcare professionals will be able to see an audit log of their own activity on the eHealth record system.

7.3.7. What about in an emergency?

Healthcare organisations participating in the eHealth record system may access a patient's eHealth record in an emergency, where patient consent is not possible. This is consistent with existing privacy laws.

In life-threatening cases where it is unreasonable or impractical to obtain a patient's consent to access the eHealth record, healthcare professionals may assert emergency access. This will override any access controls that have been set and provide your organisation with unrestricted access to a patient's eHealth record for five days. Your use of the emergency access function will be logged in the audit log and may be notified to the patient if they requested notifications.

Asserting emergency access is warranted where you believe that access to the information is necessary to lessen or prevent a serious threat to:

- an individual's life, health or safety and the patient's consent cannot be obtained. This might occur for example, if the patient is unconscious; or
- public health or public safety.

7.3.8. Can a patient enter their own health information into their eHealth record?

Only authorised healthcare professionals can enter information in the clinical section of a patient's eHeath record, ensuring it is clinically relevant and as accurate as possible.

Patients will be able to enter basic healthcare information which can be shared with healthcare professionals, and keep private notes for their own use.

7.3.9. When I view a patient's eHealth record, will there be any indication that certain documents have been classified as confidential or not readable?

If a patient has restricted your organisation's access, their eHealth record will contain a message on the provider screens that states that it is not a complete record. However, there will be no indicator on a record to tell healthcare professionals how a patient may have set their access controls or if a document has been deleted by the patient.

7.3.10. If a patient chooses to withhold information about psychiatric history, will the medications the patient may be taking be visible?

A patient is able to choose what information is viewable through their eHealth record. Just as they are able to limit access to their psychiatric information, they may also limit access to any related medications prescribed or dispensed.

7.3.11. What are my obligations if I identify an error in a patient's eHealth record?

Only authorised healthcare professionals can enter information in the clinical record, ensuring it is clinically relevant and accurate. However, if you or a patient find an error in a clinical document, you or the patient must notify the healthcare organisation from which the document originated. That organisation can then upload a corrected document.

7.3.12. Can lists of medications in the eHealth record be altered?

To maintain the integrity of the system, information uploaded to the eHealth record system, including medications, cannot be altered or edited. The system requires a new document to be uploaded, so while the old version will still be visible, the uploaded document will take precedence. If a nominated provider wishes to change the medications listed in the shared health summary, they will need to upload a new shared health summary with the updated medication information.

7.3.13. Can a patient have more than one nominated provider, e.g. a GP and a renal physician?

The nominated healthcare provider is the author of a shared health summary. There can only be one nominated provider at one time. If a patient wishes to appoint a new nominated provider, they can ask another authorised healthcare professional to author and upload their shared health summary for them. For example, a renal physician could meet the legal requirements to be a nominated provider but is unlikely to be involved in the ongoing coordinated care of the patient and may not be best suited to fulfil this role.

7.3.14. Will the eHealth record system be available on smart devices [e.g. iPad, tablet, smart phone]?

Patients will be able to view their own eHealth record on a device of their choosing. However, specific 'applications' for mobile devices such as iPads, tablets and smart phones have not been developed.

7.3.15. How will consent be managed with children?

Except in special circumstances, parents or authorised representatives will have control of their children's eHealth records from 0 to 14 years, including decisions as to which healthcare organisations have access to the child's record and which clinical documents they can see.

After a child turns 14, they will be able to choose whether to manage their own eHealth record in the same way they can apply for their own Medicare card. This includes which healthcare organisations have access to their record, which clinical documents they can see and which representatives are authorised to access to their record.

If a child chooses not to take control of their eHealth record between 14 and 17, their authorised representative[s] can continue to manage their record until they turn 18. Once an individual turns 18, authorised representative[s] will automatically lose access to their eHealth record. If an individual still wants their parent[s] or guardian[s] to view information in their eHealth record after they turn 18, they will need to take control of their record and set up nominated representatives.

In line with Department of Human Services' policy regarding the Medicare Benefits Schedule [MBS], parents will not be able to view the MBS details of children aged over the age of 14.

7.3.16 What clinical safeguards are being developed as part of the eHealth record system?

The eHealth record system is expected to improve access to clinical information and enhance patient health outcomes over time. As such, the eHealth record system has been designed with active contribution from healthcare professionals from across the health sector, key professional bodies and other quality and safety experts.

Existing clinical standards apply to the use of information sourced from the eHealth record system. Healthcare professionals can access further information about the safe use of eHealth records, including how eHealth considerations can be integrated into existing standards and clinical governance frameworks across the health sector, on the eHealth website.

7.3.17. How can I be sure that health information will be secure?

The eHealth record system implements high grade security protocols to detect and mitigate against external threats. The system will be tested frequently to ensure these mechanisms are in place and robust.

Healthcare professionals and organisations already have a duty to keep their patient's health information confidential and secure and that requirement will continue for the eHealth record system.

In addition to the limits on who can access or update an eHealth record, the eHealth record system is protected by legislation.

Security is a key design element of the system, which adheres to Australian Government security frameworks. Design features include audit trails, technology and data management controls, as well as appropriate security measures to minimise the likelihood of unauthorised access to information in a patient's record. It is important to follow the guidance available from the RACGP or your medico-legal organisation on information security.

The Australian Government strongly encourages businesses and organisations to take steps to ensure they are operating safely or providing services securely online. The Australian Government's website Stay Smart Online offers a lot of useful advice and tips for small and medium businesses about IT security.

8. Helpdesk Contact Details

	Description	Helpdesk Contact	Hours of Operation	Information and Assistance
1	Understand the ePIP Requirement	ePIP enquiry line: **phone:** 1800 222 032 **email:** pip@humanservices.gov.au	8:30am – 5:00pm [ACST] Monday - Friday	• ePIP requirements • ePIP Application Process
2	Review the ePIP Product Register	Online enquiry form: **web:** https://epipregister.nehta.gov.au/enquiry	8:00am – 5:00pm [QLD] Monday - Friday	• Information on your software vendor[s] conformance with the ePIP requirements
3	Register for a Seed HPI-O	HI Service enquiry line” **phone:** 1300 361 457 **email:** healthcareidentifiers@humanservices.gov.au	8:30am – 5:00pm [EST] Monday - Friday	• HI Service general information and questions • Completing Seed Organisation HPI-O Applications • Registering or updating an ROs/OMOs details
4	Register for the PCEHR Sign the PCEHR Participation Agreement	PCEHR enquiry line: **phone:** 1800 723 471	8:30am – 5:00pm [EST] Monday - Friday	• PCEHR general information and questions • Completing PCEHR Applications • Completing PCEHR Participation Agreements

	Description	Helpdesk Contact	Hours of Operation	Information and Assistance
5	Register for a NASH PKI Certificate for Healthcare Provider Organisation Apply/Renew a Human Services PKI Site Certificate [if required]	eBusiness Service Centre: **phone:** 1800 700 199 [option 2]	8:30am – 5:00pm [EST] Monday - Friday	• eHealth Record PKI general information and questions • NASH PKI general information and questions • Medicare Location PKI Certificates general information and questions • Completing NASH PKI Certificate for Healthcare Provider Organisations Applications • PKI Certificates installation support • PKI Certificate and Tokens lost / forgotten passwords
6	Complex Seed and Network Organisation HPI-O Structures Secure Message Delivery [SMD]	Nehta Helpdesk: **email:** nehtasupport@nehta. gov.au **phone:** 1300 901 001	8:00am – 5:00pm [QLD] Monday - Friday	• Seed and Network structure questions • Questions relating to secure message delivery [SMD]

8.1. Related Resources

The following is a list of information resources that you may find useful for introductory or other reference purposes on eHealth generally and on the national eHealth program specifically. It is not essential that you read through all of these at this point in time, as many are referred to later in the guide itself.

Resource	Website
Australian Government's web-sites, which have information, including brochures, on eHealth, and the ability to subscribe for updates and notification of key events	http://www.ehealth.gov.au
Introduction to the eHealth record system for healthcare professionals	http://publiclearning.ehealth.gov.au/modules/hcpIntro/index.html a Learning Module
Department of Health and Ageing's website on eHealth	http://www.health.gov.au/internet/main/publishing.nsf/Content/eHealth
Healthcare Identifiers Act 2010	http://www.comlaw.gov.au/Details/C2010C00440
Healthcare Identifiers [Consequential Amendments] Act 2010	http://www.comlaw.gov.au/Details/C2010A00073
Healthcare Identifiers Regulations 2010	http://www.comlaw.gov.au/Details/F2010L01829
DHS web-site for healthcare providers. Includes information and resources about the HI Service	http://www.medicareaustralia.gov.au/provider/ http://www.medicareaustralia.gov.au/provider/health-identifier/
DHS web-site for individuals	http://www.humanservices.gov.au/customer/services/medicare/healthcare-identifiers-service
RACGP's eHealth web-site. Includes resources on clinical governance, quality improvement and computer security	http://www.racgp.org.au/ehealth

Resource	Website
The AMA's Guide to Using the PCEHR [Draft available]	Draft is available at http://ama.com.au/node/7648
The eHealthAus YouTube Channel that includes videos demonstrating many features and benefits of eHealth	http://www.youtube.com/user/eHealthAus
NEHTA web-site to support General Practice	http://www.nehta.gov.au/registration-support-general-practice
NEHTA web-site for Healthcare Identifiers	http://www.nehta.gov.au/connectingaustralia/healthcare-identifiers
The NEHTA Model Healthcare Community web-site. Includes a video that shows how the Healthcare Identifier Service will work.	http://www.nehta.gov.au/connectingaustralia/healthcare-identifiers/discover-themodel-healthcare-community

9. Key Definitions

Key Definition	Description
Authorisation links	An authorisation link connects a healthcare professional to an organisation so that an authorised individual can access the eHealth record via the provider portal on behalf of their organisation. Authorisation links only apply for organisations that want their healthcare professionals to use the provider portal. Authorisation links do not need to be created for healthcare professionals who use a conformant clinical information system to access the eHealth record system to view a consumer's eHealth record.
eHealth Record Individual Public Key infrastructure PKI Individual certificate	The eHealth Record PKI provides digital certificates for healthcare providers to authenticate to, and access, the eHealth Record system. An individual healthcare provider MUST have a Department of Human Services eHealth Record Individual Public Key Infrastructure [PKI] certificate.
Electronic transfer of prescriptions [ETP]	Electronic prescriptions are sent from your clinical software system to a Prescription Exchange Service [PES] where prescriptions are stored, and can be retrieved later by a dispenser at the time of dispensing.
Healthcare Identifiers Service	The HI Service provides a consistent set of identifiers for healthcare individuals [consumers] and healthcare providers [organisations and individual professionals]. The HI Service enables providers to link health information and data to the right consumer in a secure, consistent and accurate manner.
Healthcare Organisation	An organisation that has conducted, conducts, or will conduct, an enterprise that provides healthcare.
Health Provider Identifier [HPI-I]	A HPI-I is a unique 16-digit number that is allocated by the Healthcare Identifier [HI] Service to the provider. It ensures that providers can be identified. A HPI-I is required to access the HI Service and eHealth record.
Health Provider Identifier – Organisation [HPI-O]	A HPI-O is a number that uniquely identifies organisations where healthcare has been provided.
Individual Healthcare Identifiers [IHI]	An individual healthcare identifier [IHI] is a unique 16-digit number used to assist health providers communicate health information about an individual. An IHI provides a reliable and accurate way of uniquely identifying a person to provides healthcare and manage healthcare records.

Key Definition	Description
National authentication service for health public key infrastructure certificate for healthcare provider organisations [NASH PKI digital certificate]	The NASH PKI provides digital certificates for healthcare providers to authenticate to, and access, the eHealth Record systems and for authenticating or protection of confidentiality, and integrity of electronic communications with other Organsiations [and/or their information technology providers where applicable]. This certificate can ONLY be used to connect to the eHealth record system and for secure sending of electronic messages to other healthcare provider organisations. The certificate cannot be used for accessing the HI services or online Medicare claiming channels.
Nominated provider	A nominated provider is the individual healthcare professional who agrees with you to develop and manage your shared health summary. For most people, the nominated provider is likely to be your GP – this is because your GP is usually the person most involved in your ongoing, coordinated care. A nominated provider is decided by mutual agreement; if you wish to change nominated providers you can agree this with another doctor or authorised healthcare professional. You do not need to have a nominated provider in order to have an eHealth record.
Organisational Maintenance Officer [OMO]	An organisation maintenance officer is registered under the HI service and has authority to act on behalf of a network organisation in its dealings with the System Operator of the eHealth record system. A seed organisation maintenance officer has authority to act on behalf of the seed organisation. A healthcare organisation can have multiple organisation maintenance officers.
PCEHR	Personally controlled electronic health record is a secure, voluntary electronic record.
PCEHR compliant digital credentials	PCEHR compliant digital credentials are used to authenticate system access and are part of the security measures put in place for the eHealth record system. PCEHR compliant digital credentials can only be obtained by healthcare organisations and individuals who are registered with the HI Service.

Key Definition	Description
PKI organisation certificate	A PKI acts as a secure electronic signature and enables the secure exchange of data by ensuring: 1. Authentication - disclosing the sender of the message 2. Integrity – ensures the message has not been altered 3. Non-repudiation – the sender cannot dispute the creation or sending the message 4. Confidentiality – only the person that is designated to receive the message can open it. A PKI organisation certificate used for Medicare purposes can be HI enabled
Responsible Officer [RO]	A responsible officer is registered under the HI service and has authority to act on behalf of the seed organisation and relevant network organisations in its dealings with the System Operator. For large organisations, the responsible officer is usually the chief executive officer or chief operations officer, and for small organisations the responsible officer is usually a practice manager or the business owner.
Secure Messaging Delivery [SMD]	eHealth combines the basic technologies of unique identification, authorisation and message security to provide the safest and optimally secure method of exchanging healthcare information. These technologies, known collectively as secure messaging, ensure that the health information exchanged by healthcare providers is protected against malicious interference.
Seed Organisation	A seed organisation, for the purpose of participating in the eHealth record system, is a legal entity that provides or controls the delivery of healthcare services.
System Operator	This is the person with responsibility for establishing and operating the eHealth record system. From the start of the eHealth record system, this is the Secretary of the Department of Health and Ageing. Customer service officers from the Department of Human Services will undertake some of the eHealth record system's day-to-day tasks on behalf of the System Operator.

10. Acronyms and Abbreviations

ACSQHS	Australian Commission on Safety and Quality in Healthcare
AGPN	Australian General Practice Network – from 1 July 2012 to be known as Australian Medicare Local Network
AHPRA	Australian Health Practitioner Regulation Agency
AMA	Australian Medical Association
AMLN	Australian Medicare Local Network
CDA	Clinical Document Architecture
CDSA	Clinical Data Self Assessment
DHS	Commonwealth Department of Human Services, formally known as Medicare
DoHA	Commonwealth Department of Health & Ageing
DAO	Duly Authorised Officer
GP	General Practitioner
HI	Healthcare Identifiers
HI Service	Healthcare Identifiers Service
HI Service Operator	Commonwealth Department of Human Services [DHS]
HL7	Health Level Seven
HPD	Healthcare Provider Directory
HPI-I	Healthcare Provider Identifier - Individual
HPI-O	Healthcare Provider Identifier - Organisation
HPOS	Health Professional Online Services
IHI	Individual Healthcare Identifier
LHN	Local Health Network

ML	Medicare local
NASH	National Authentication Service for Health
NEHTA	National e-Health Transition Authority
OMO	Organisation Maintenance Officer
PCEHR	Personally Controlled Electronic Health Record, now known as National Electronic Health Record
PKI	Public Key Infrastructure
RO	Responsible Officer
SHS	Shared Health Summary
SMD	Secure Message Delivery
RACGP	Royal Australian College of General Practitioners